7/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

013183164 **Image available**
WPI Acc No: 2000-355037/ **200031**
XRPX Acc No: N00-266141
Prepaid electronic cash system indicates praxis of settlement-of-accounts to settlement-of-accounts processor based on account number of payment system
Patent Assignee: SONY CORP (SONY)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000113085	A	20000421	JP 98286341	A	19981008	200031	B

Priority Applications (No Type Date): JP 98286341 A 19981008
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000113085	A		19	G06F-019/00	

Abstract (Basic): **JP 2000113085** A
NOVELTY - A settlement-of-accounts unit (55) shows settlement-of-accounts to a payment system. User management unit (35) manages account number of user's payment system. A communication unit (37) shows changes in balance of prepayment of user, based on identification information of the user. The praxis of settlement-of-accounts is indicated to settlement-of-accounts processor based on account of payment system.
DETAILED DESCRIPTION - An account management unit (45) stores information which identifies the user and balance money of the user on the basis of prepayment money. The encryption is performed by user's payment system with disclosure key information which identifies user and a settlement-of-accounts processor.
USE - Prepaid electronic cash system for processing money to be paid.
ADVANTAGE - The praxis of the settlement-of-accounts is indicated to a settlement-of-accounts processor on the basis of account number of payment system. Therefore, the necessity for managing a special apparatus by the user is eliminated. Utilization of cash is performed safely.
DESCRIPTION OF DRAWING(S) - The figure shows the components of prepaid electronic cash system.
User management unit (35)
Communication unit (37)
Account management unit (45)
Settlement-of-accounts unit (55)
pp; 19 DwgNo 1/9
Title Terms: PREPAYMENT; ELECTRONIC; CASH; SYSTEM; INDICATE; SETTLE; ACCOUNT; SETTLE; ACCOUNT; PROCESSOR; BASED; ACCOUNT; NUMBER; PAY; SYSTEM
Derwent Class: P85; T01; T05
International Patent Class (Main): G06F-019/00
International Patent Class (Additional): G06F-017/60; G07F-019/00; G09C-001/00
File Segment: EPI; EngPI

7/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06527364 **Image available**
ELECTRONIC CASH SYSTEM

PUB. NO.: 2000-113085 A]

PUBLISHED: April 21, 2000 (20000421)
INVENTOR(s): MATSUYAMA SHINAKO
APPLICANT(s): SONY CORP
APPL. NO.: 10-286341 [JP 98286341]
FILED: October 08, 1998 (19981008)
INTL CLASS: G06F-019/00; G06F-017/60; G07F-019/00; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To make usable electronic cash in safety without requiring any special device, to disable individual information and individual purchase information to be grasped unnecessarily, and to make the detectable an illegal act and controllable over the circulation of money.

SOLUTION: An account management part 45 stores information for identifying users and the amounts of money spent by the users on a prepayment basis. An adjustment part 55 instructs a payment institution to settle the accounts. A user management part 35 manages the information for identifying the users and the account numbers of the users at he payment institution which are ciphered with an open key of a settlement processor and a communication part 37 indicates alterations of the balances of prepayment of the users stored in an account management device according to the information for identifying the users and instructs the settlement processor to settle the accounts.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－113085
（P2000－113085A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	３６０	３Ｅ０４０
17/60		Ｇ０９Ｃ　1/00	６４０Ａ	５Ｂ０４９
Ｇ０７Ｆ　19/00			６６０Ｃ	５Ｂ０５５
Ｇ０９Ｃ　1/00	６４０		６６０Ｇ	
	６６０	Ｇ０６Ｆ　15/21	３４０Ａ	

審査請求　未請求　請求項の数３　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願平10－286341

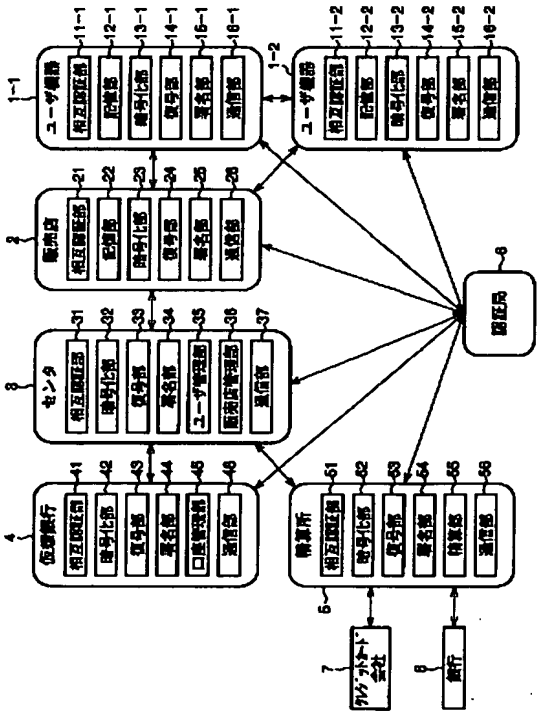
(22)出願日　平成10年10月８日(1998.10.8)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　松山　科子
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　電子現金システム

(57)【要約】
【課題】　特殊な装置を必要とせず、安全に電子現金の利用ができ、個人の情報および個人の購入情報が不必要に把握できず、不正の検出および金銭の流通が管理できるようにする。
【解決手段】　口座管理部４５は、利用者を識別する情報および前払いの代金を基にした利用者の利用金額を記憶する。精算部５５は、支払機関に決済を指示する。ユーザ管理部３５は、利用者を識別する情報および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理し、通信部３７は、利用者を識別する情報を基に、口座管理装置が記憶する利用者の前払いの残高の変更を指示し、支払い機関の口座番号を基に、決済処理装置に決済の実行を指示する。



【特許請求の範囲】
【請求項１】　口座管理装置、決済処理装置、および制御装置からなる、前払いにより代金の支払いを処理する電子現金システムにおいて、
前記口座管理装置は、
利用者を識別する情報、および前記前払いの代金を基にした前記利用者の利用金額を記憶する記憶手段を備え、
前記決済処理装置は、
支払機関に決済を指示する決済指示手段を備え、
前記制御装置は、
利用者を識別する情報、および前記決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理する管理手段と、
前記管理手段が管理する前記利用者を特定する情報を基に、前記口座管理装置の前記記憶手段が記憶する前記利用者の前記前払いの残高の変更を指示する残高変更指示手段と、
前記管理手段が管理する前記支払い機関の口座番号を基に、前記決済処理装置の前記決済指示手段に決済の実行を指示する決済実行指示手段とを備えることを特徴とする電子現金システム。
【請求項２】　前記口座管理装置、決済処理装置、および制御装置は、通信の前に所定の相互認証処理を実行することを特徴とする請求項１に記載の電子現金システム。
【請求項３】　前記口座管理装置、決済処理装置、および制御装置の間で送信されるデータは、暗号化されていることを特徴とする請求項１に記載の電子現金システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子現金システムに関し、特に、前払いにより代金の支払いを処理する電子現金システムに関する。
【０００２】
【従来の技術】電子現金システムの現金の管理方式は、耐タンパー性のある機器を利用し、残高が改竄出来ないことを前提とし、残高を管理する「残高管理方式」と、センターで発行した現金のIDを管理し、二重使用されていないかのチェックを行うために、電子現金に、額面および識別番号を持たせる「電子紙幣方式」に大別される。
【０００３】電子現金システムを実用に供するためには、ユーザの個人情報および購入情報に対する匿名性、並びに任意のユーザ機器および販売店などの間で金銭の移動が可能なオープンループ型流通の実現が必要である。
【０００４】電子現金システムで、上記の要件を満足しているのは、Mondex（商標）のみである。Mondexでは、サービスを受けるユーザ機器、および商品を提供する販売店は、それぞれMondexカードを保持し、販売店はさらに、Mondexカードを読み書きするための特殊な装置が必要であり、それを用いて電子現金の入出金を行う。
【０００５】インターネット上でのMondexの利用の安全性は、暗号モジュールを常に２つ用意し、安全が保証される方に切り替えて利用するなど、安全性を強化したMondexカードの安全性に依存している。また、Mondexのシステムは、取り引き情報を一切管理しないため、個人の情報および購入履歴は、その匿名性が保たれる。
【０００６】
【発明が解決しようとする課題】しかしながら、Mondexのシステムでは、販売店は、特殊な装置を管理する必要があり、手間がかかる。また、取り引き情報を一切管理しないため、不正利用があった際、その検出は出来きず、さらに、金銭の流通が、管理出来ない。
【０００７】本発明はこのような状況に鑑みてなされたものであり、特殊な装置を管理する必要がなく、安全に電子現金の利用ができ、個人の情報および個人の購入情報を各装置が不必要に把握できず、不正の検出が可能で、金銭の流通が管理できるようにすることを目的とする。
【０００８】
【課題を解決するための手段】請求項１に記載の電子現金システムは、口座管理装置が、利用者を識別する情報、および前払いの代金を基にした利用者の利用金額を記憶する記憶手段を備え、決済処理装置が、支払機関に決済を指示する決済指示手段を備え、制御装置が、利用者を識別する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理する管理手段と、管理手段が管理する利用者を特定する情報を基に、口座管理装置の記憶手段が記憶する利用者の前払いの残高の変更を指示する残高変更指示手段と、管理手段が管理する支払い機関の口座番号を基に、決済処理装置の決済指示手段に決済の実行を指示する決済実行指示手段とを備えることを特徴とする。
【０００９】請求項１に記載の電子現金システムにおいては、口座管理装置が、利用者を識別する情報、および前払いの代金を基にした利用者の利用金額を記憶し、決済処理装置が、支払機関に決済を指示し、制御装置が、利用者を識別する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理し、利用者を特定する情報を基に、口座管理装置が記憶する利用者の前払いの残高の変更を指示し、支払い機関の口座番号を基に、決済処理装置に決済の実行を指示する。
【００１０】
【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但

し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１１】すなわち、請求項１に記載の電子現金システムは、口座管理装置（例えば、図１の仮想銀行４）が、利用者を特定する情報、および前払いの代金を基にした利用者の利用金額を記憶する記憶手段（例えば、図１の口座管理部４５）を備え、決済処理装置（例えば、図１の精算所５）が、支払機関に決済を指示する決済指示手段（例えば、図１の精算部５５）を備え、制御装置（例えば、図１のセンター３）が、利用者を特定する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理する管理手段（例えば、図１のユーザ管理部３５）と、管理手段が管理する利用者を特定する情報を基に、口座管理装置の記憶手段が記憶する利用者の前払いの残高の変更を指示する残高変更指示手段（例えば、図１の通信部３７）と、管理手段が管理する支払い機関の口座番号を基に、決済処理装置の決済指示手段に決済の実行を指示する決済実行指示手段（例えば、図１の通信部３７）とを備えることを特徴とする。

【００１２】図１は、本発明を適用した電子現金システムの構成を表す図である。ユーザ機器１－１は、販売店２から、商品を購入し、またはサービスを受け、センター３、仮想銀行４、および精算所５を介して、販売店２に代金を支払う。ユーザ機器１－２は、販売店２から、商品を購入し、またはサービスを受け、センター３、仮想銀行４、および精算所５を介して、販売店２に代金を支払う。販売店２は、ユーザ機器１－１または１－２に商品またはサービスを提供し、センター３、仮想銀行４、および精算所５を介して、ユーザ機器１－１またはユーザ機器１－２から代金を受け取る。センター３は、ユーザ機器１－１、ユーザ機器１－２、および販売店２の所定のデータを記憶し、ユーザ機器１－１、ユーザ機器１－２、および販売店２の決済処理を精算所５に実行させる。仮想銀行４は、電子マネーを発行する機関であり、電子マネーの発行単位（ユーザ機器１－１または１－２並びに販売店２）のIDを発行し、IDに対応する残高、または売り上げ金額などを管理する。精算所５は、銀行８またはカード会社７に対して、ユーザ機器１－１または１－２並びに販売店２の口座毎またはカード番号毎に、出金または入金の手続を実行する。認証局６は、ユーザ機器１－１乃至精算所５の要求に対応し、所定のデータを含んだ証明書を発行する。

【００１３】ユーザ機器１－１の相互認証部１１－１は、ユーザ機器１－２、販売店２、センター３、または認証局６と、後述する処理で相互認証する。記憶部１２－１は、耐タンパー性を有する素子から構成され、電子マネーのユーザID、残高、および未精算金額を記憶する。暗号化部１３－１は、ユーザ機器１－２、販売店２、またはセンター３に送信する、購入金額、購入品情報、および電子マネーのユーザIDなどの所定のデータを暗号化する。復号部１４－１は、ユーザ機器１－２、販売店２、センター３、または認証局６から受信する、ユーザID、金額、および残高などの暗号化された情報を復号する。署名部１５－１は、ユーザ機器１－２、販売店２、センター３、または認証局６に送信する、購入金額、購入品情報、および電子マネーのユーザIDなどの所定のデータにハッシュ関数を適用してハッシュ値を算出し、所定の鍵で暗号化し、署名を作成する。署名部１５－１はまた、ユーザ機器１－２、販売店２、センター３、または認証局６から受信する、データおよびデータに付された署名を検査し、改竄がなかったか否か判定する。通信部１６－１は、ユーザ機器１－２、販売店２、センター３、または認証局６に所定のデータを送信し、ユーザ機器１－２、販売店２、センター３、または認証局６から送信されたデータを受信する。

【００１４】ユーザ機器１－２の相互認証部１１－２、記憶部１２－２、暗号化部１３－２、復号部１４－２、署名部１５－２、および通信部１６－２は、ユーザ機器１－１の相互認証部１１－１、記憶部１２－１、暗号化部１３－１、復号部１４－１、署名部１５－１、および通信部１６－１と同様であり、その説明は省略する。なお、以下、特に区別する必要が無いときは、ユーザ機器１－１、ユーザ機器１－２を、単に、ユーザ機器１と称する。

【００１５】販売店２の相互認証部２１、センター３の相互認証部３１、仮想銀行４の相互認証部４１、および精算所５の相互認証部５１は、ユーザ機器１－１の相互認証部１１－１と同様の処理を行うのでその説明は省略する。

【００１６】販売店２の暗号化部２３、センター３の暗号化部３２、仮想銀行４の暗号化部４２、および精算所５の暗号化部５２は、ユーザ機器１－１の暗号化部１３－１と同様の処理を行うのでその説明は省略する。

【００１７】販売店２の復号部２４、センター３の復号部３３、仮想銀行４の復号部４３、および精算所５の復号部５３は、ユーザ機器１－１の復号部１４－１と同様の処理を行うのでその説明は省略する。

【００１８】販売店２の署名部２５、センター３の署名部３４、仮想銀行４の署名部４４、および精算所５の署名部５４は、ユーザ機器１－１の署名部１５－１と同様の処理を行うのでその説明は省略する。

【００１９】販売店２の通信部２６、センター３の通信部３７、仮想銀行４の通信部４６、および精算所５の通信部５６は、ユーザ機器１－１の通信部１６－１と同様の処理を行うのでその説明は省略する。

【００２０】販売店２の記憶部２２は、耐タンパー性を有する素子から構成され、販売店ID、および売り上げ金額などを記憶する。

【００２１】センター３のユーザ管理部３５は、ユーザ

IDに対応するユーザの公開鍵Ｋｐｕ、および精算所５の公開鍵Ｋｐｐｇで暗号化したユーザのクレジットカード番号を記憶し、管理する。センター３の販売店管理部３６は、販売店IDに対応する販売店２の公開鍵Ｋｐｍ、および精算所５の公開鍵Ｋｐｐｇで暗号化した販売店２の口座番号を記憶し、管理する。

【００２２】仮想銀行４の口座管理部４５は、ユーザIDに対応するユーザの電子現金の残高、および販売店IDに対応する販売店２の売り上げ金額を記憶する。

【００２３】精算所５の精算部５５は、ユーザ機器１－１または１－２並びに販売店２の口座毎に、銀行８またはカード会社７に対して、出金または入金の手続を指示する。

【００２４】ユーザ機器１が、仮想銀行４に初めて入金し、ユーザIDを登録するときの処理を、図２のフローチャートを用いて説明する。ステップＳ１１において、ユーザ機器１の通信部１６は、認証局６に個人情報、口座情報、およびユーザ機器１の公開鍵Ｋｐｕを送信する。認証局６は、ユーザ機器１の通信部１６が送信したデータを受信する。ステップＳ１２において、認証局６は、受信した個人情報、口座情報、およびユーザ機器１の公開鍵Ｋｐｕに所定のハッシュ関数を適用し、得られたハッシュ値を認証局６の秘密鍵Ｋｓｃａで暗号化して署名を作成し、個人情報、口座情報、およびユーザ機器１の公開鍵Ｋｐｕに付加して証明書を作成し、ユーザ機器１に送信する。ユーザ機器１の通信部１６は、認証局６が送信したデータを受信する。

【００２５】署名は、データまたは証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【００２６】ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【００２７】署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4，MD5，SHA-1などが用いられる。

【００２８】次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００２９】公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるpおよびqを求め、さらにpとqの積であるｎを求める。(p-1)と(q-1)の最小公倍数Lを算出し、更に、３以上L未満で、かつ、Ｌと互いに素な数eを求める（すなわち、eとLを共通に割り切れる数は、１のみである）。

【００３０】次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわち、d，e、およびLの間には、ed=1 mod Lが成立し、dはユークリッドの互除法で算出できる。このとき、nとeが公開鍵とされ、p,q,およびdが、秘密鍵とされる。

【００３１】暗号文Cは、平文Mから、式（１）の処理で算出される。

C=M^e mod n　　(1)

【００３２】暗号文Cは、式（２）の処理で平文Mに、復号される。

M=C^d mod n　　（２）

【００３３】証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

M=C^d=(M^e)^d=M^(ed) mod n　　（３）

【００３４】秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００３５】また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線y^2=x^3+ax+b上の、ある点をBとする。楕円曲線上の点の加算を定義し、nBは、Bをn回加算した結果を表す。同様に、減算も定義する。BとnBからnを算出することは、困難であることが証明されている。BとnBを公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式（４）および式（５）の処理で算出される。

C1=M+rnB　　（４）

C2=rB　　（５）

【００３６】暗号文C1およびC2は、式（６）の処理で平

文Mに、復号される。

M=C1-nC2　（６）

【００３７】復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００３８】ステップＳ１３において、ユーザ機器１の相互認証部１１は、センター３の相互認証部３１と、相互認証し、後述する乱数の連接Ｒ２‖Ｒ３をセンター３とユーザ機器１の間の一時鍵Ｋｔｓｕとして共有する。相互認証の手続については、図３のフローチャートを用いて、後述する。ステップＳ１４において、ユーザ機器１の暗号化部１３は、精算所５の公開鍵Ｋｐｐｇでユーザの予め記憶しているクレジットカード番号を暗号化し、署名部１５は、ユーザ機器により設定された電子現金発行金額に署名を付す。ユーザ機器１の暗号化部１３は、暗号化されたクレジットカード番号および署名を付された電子現金発行金額を一時鍵Ｋｔｓｕで暗号化し、通信部１６は、精算所５の公開鍵Ｋｐｐｇで暗号化され、一時鍵Ｋｔｓｕで暗号化されたクレジットカード番号、および署名を付され、一時鍵Ｋｔｓｕで暗号化された電子現金発行金額をセンター３に送信する。センター３の通信部３７は、ユーザ機器１から送信された、クレジットカード番号、および電子現金発行金額を受信する。

【００３９】ステップＳ１５において、センター３の復号部３３は、一時鍵Ｋｔｓｕで暗号化されたクレジットカード番号および電子現金発行金額を復号し、署名部３４は、電子現金発行金額に付された署名を、後述する相互認証で得られたユーザ機器１の証明書に含まれるユーザ機器の公開鍵Ｋｐｕで、復号部３３に復号させ得られた値と、一時鍵Ｋｔｓｕで復号した電子現金発行金額にハッシュ関数を適用して得られたハッシュ値とを比較し、同一であれば電子現金発行金額が改竄されていないと判定する。電子現金発行金額が改竄されていると判定された場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップＳ１６に進み、センター３の相互認証部３１は、精算所５の相互認証部５１と相互認証し、センター３と精算所５の間の一時鍵Ｋｔｓｐを共有する。相互認証の手続については、図３のフローチャートを用いて、後述する。ステップＳ１７において、センター３の署名部３４は、電子現金発行金額に署名を付し、暗号化部３２は、ユーザ機器１の証明書、精算所５の公開鍵Ｋｐｐｇで暗号化されたクレジットカード番号、並びにセンター３の署名およびユーザ機器１の署名を付した電子現金発行金額を一時鍵Ｋｔｓｐで暗号化し、通信部３７は、暗号化されたデータを精算所５に送信する。精算所５の通信部５６は、センター３から送信されたデータを受信する。

【００４０】ステップＳ１８において、精算所５の復号部５３は、センター３から受信したデータを一時鍵Ｋｔｓｐで復号し、精算所５の署名部５４は、電子現金発行金額に付されたセンター３の署名およびユーザ機器１の署名を検証し、電子現金発行金額に改竄がないことを確認する。署名の検証の処理は、ステップＳ１５における場合と同様であるので、その説明は省略する。署名部３４が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップＳ１９に進み、署名部５４は、受信したクレジットカード番号にハッシュ関数を適用してハッシュ値を算出し、証明書にあるハッシュ値と一致するかを検証し、クレジットカード番号に改竄がないことを確認する。署名部３４がクレジットカード番号の改竄を発見した場合、処理は終了する。クレジットカード番号が改竄されていない場合、ステップＳ２０に進み、精算部５５は、通信部５６を介して、クレジットカード会社７に、与信および引き落とし命令を送付する。

【００４１】ステップＳ２１において、署名部５４は、ステップＳ１８およびステップＳ１９の検証結果並びにステップＳ２０の処理結果に署名を付し、暗号化部５２は、署名を付した検証結果および処理結果を暗号化し、通信部５６は、暗号化した検証結果および処理結果をセンター３に送信する。センター３の通信部３７は、精算所５が送信した検証結果および処理結果を受信し、復号部３３は、精算所５から受信した検証結果および処理結果を復号する。受信した検証結果が不正があったことを示し、および処理結果が正常に終了しなかったことを示している場合、処理は終了する。

【００４２】ステップＳ２１で受信した検証結果が不正がないことを示し、および処理結果が正常に終了したことを示している場合、ステップＳ２２において、センター３の相互認証部３１は、仮想銀行４の相互認証部４１と相互認証し、センター３と仮想銀行４の間で一時鍵Ｋｔｓｂを共有する。相互認証の手続については、図３のフローチャートを用いて、後述する。ステップＳ２３において、暗号化部３２は、ユーザ機器１の証明書、並びにステップＳ１７で作成した、センター３の署名およびユーザ機器１の署名を付した電子現金発行金額を一時鍵Ｋｔｓｂで暗号化し、通信部３７は、暗号化された、ユーザ機器１の証明書および電子発行金額を仮想銀行４に送信する。仮想銀行４の通信部４６は、センター３から送信されたユーザ機器１の証明書および電子発行金額を受信する。

【００４３】ステップＳ２４において、仮想銀行４の復号部４３は、センター３から受信したユーザ機器１の証明書および電子発行金額を一時鍵Ｋｔｓｂで復号し、署名部４４は、電子現金発行金額に付されたセンター３の署名およびユーザ機器１の署名を検証し、電子現金発行金額に改竄がないことを確認する。署名の検証の処理は、ステップＳ１５における場合と同様であるので、そ

の説明は省略する。署名部４４が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップＳ２５において、仮想銀行４の口座管理部４５は、ユーザIDを生成し、ユーザIDに対応させ、電子現金発行金額を記憶する。ステップＳ２６において、署名部４４は、ユーザIDに署名を付して、暗号化部４２は、ユーザIDを一時鍵Ｋｔｓｂで暗号化し、通信部４６は、センター３に暗号化したユーザIDを送信する。センター３の通信部３７は、仮想銀行４が送信したユーザIDを受信する。

【００４４】ステップＳ２７において、センター３の復号部３３は、仮想銀行４が送信したユーザIDを一時鍵Ｋｔｓｂで復号し、ユーザ機器管理部３５は、復号したユーザID、ステップＳ１３で受信したユーザ機器の公開鍵Ｋｐｕ、およびステップＳ１４で受信した精算所５の公開鍵Ｋｐｐｇで暗号化したクレジットカード番号の組を記憶し、管理する。ステップＳ２８において、センター３の署名部３４は、ユーザIDに署名を付して、暗号化部３２は、一時鍵Ｋｔｓｕでユーザを暗号化し、通信部３７は、暗号化したユーザIDをユーザ機器に送信する。ユーザ機器１の通信部１６は、センター３が送信したユーザIDを受信する。

【００４５】ステップＳ２９において、ユーザ機器１の復号部１４は、受信したユーザIDを一時鍵Ｋｔｓｕで復号し、記憶部１２は、ステップＳ２８で受信したユーザIDおよびステップＳ１４で送信した電子現金発行金額を電子現金残高として記憶する。

【００４６】このように、ユーザ機器１は、初めての入金で、仮想銀行４に、ユーザIDが登録され、ユーザIDと対応して先払いした金額と同額の電子現金発行金額が記憶される。

【００４７】図２のステップＳ１３における、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、ユーザ機器１の相互認証部１１とセンター１の相互認証部３１との相互認証の処理を、図３のフローチャートを用いて説明する。ステップＳ４１において、ユーザ機器１の相互認証部１１は、６４ビットの乱数Ｒ１を生成する。ステップＳ４２において、ユーザ機器１の相互認証部１１は、自分自身の公開鍵Ｋｐｕを含む証明書（認証局６からステップＳ１２で取得したもの）と、乱数Ｒ１をセンター３の相互認証部３１に送信する。

【００４８】ステップＳ４３において、センター３の相互認証部３１は、受信した証明書の署名（認証局６の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、ユーザ機器１の公開鍵Ｋｐｕとユーザ機器１の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているユーザ機器１の公開鍵Ｋｐｕおよびユーザ機器１の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｕおよびユーザ機器１の名前のハッシュ値は、平文のまま証明書に格納されていたユーザ機器１の公開鍵Ｋｐｕおよびユーザ機器１の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｕが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なユーザ機器でないことになる。この時処理は終了される。

【００４９】適正な認証結果が得られたとき、ステップＳ４４において、センター３の相互認証部３１は、６４ビットの乱数Ｒ２を生成する。ステップＳ４５において、センター３の相互認証部３１は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ４６において、センター３の相互認証部３１は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ４７において、センター３の相互認証部３１は、連接Ｒ１‖Ｒ２を、ステップＳ４３で取得したユーザ機器１の公開鍵Ｋｐｕで暗号化する。ステップＳ４８において、センター３の相互認証部３１は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｕで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をユーザ機器１の相互認証部１１に送信する。

【００５０】ステップＳ４９において、ユーザ機器１の相互認証部１１は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ４３における場合と同様であるので、その説明は省略する。ステップＳ５０において、ユーザ機器１の相互認証部１１は、センター３の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ４９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ５１において、ユーザ機器１の相互認証部１１は、自分自身の公開鍵Ｋｐｕで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｕで復号する。ステップＳ５２において、ユーザ機器１の相互認証部１１は、ステップＳ５０で復号された連接Ｒ１‖Ｒ２と、ステップＳ５１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればセンター３を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【００５１】適正な認証結果が得られたとき、ステップＳ５３において、ユーザ機器１の相互認証部１１は、６４ビットの乱数Ｒ３を生成する。ステップＳ５４において、ユーザ機器１の相互認証部１１は、ステップＳ５０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ５５において、ユーザ機器１の相互認証部１１は、連接Ｒ２‖Ｒ３を、ステップＳ４９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ５６において、ユーザ機器１の相互認証部１１

は、暗号化した連接Ｒ２‖Ｒ３をセンター３の相互認証部３１に送信する。

【００５２】ステップＳ５７において、センター３の相互認証部３１は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ５８において、センター３の相互認証部３１は、復号した乱数Ｒ２が、ステップＳ４４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、ユーザ機器１を適正なユーザ機器として認証し、一致しなければ、不適正なユーザ機器として、処理を終了する。

【００５３】以上のように、センター３の相互認証部３１とユーザ機器１の相互認証部１１は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵として利用される。

【００５４】ユーザ機器１が、仮想銀行４に２回目以降に入金するときの処理を、図４のフローチャートを用いて説明する。ステップＳ７１において、ユーザ機器１の相互認証部１１は、センター３の相互認証部３１と、相互認証し、センター３とユーザ機器１の間の一時鍵Ｋｔｓｕを共有する。相互認証の手続は、図３で説明したものと同様であり、その説明は省略する。ステップＳ７２において、ユーザ機器１の署名部１５は、ユーザIDに署名を付し、電子現金発行金額に署名を付す。ユーザ機器１の暗号化部１３は、署名を付されたユーザIDおよび署名を付された電子現金発行金額を一時鍵Ｋｔｓｕで暗号化し、通信部１６は、一時鍵Ｋｔｓｕで暗号化されたユーザIDおよび電子現金発行金額をセンター３に送信する。センター３の通信部３７は、ユーザ機器１から送信された、一時鍵Ｋｔｓｕで暗号化されたユーザIDおよび電子現金発行金額を受信する。

【００５５】ステップＳ７３において、センター３の復号部３３は、一時鍵Ｋｔｓｕで暗号化されたユーザIDおよび電子現金発行金額を一時鍵Ｋｔｓｕで復号し、署名部３４は、復号して得られた、電子現金発行金額に付された署名を検証し、電子現金発行金額が改竄されていないことを確認する。署名の検証は、図２のステップＳ１５で説明した処理と同様なので、その説明は省略する。署名部３４が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップＳ７４に進み、センター３のユーザ管理部３５は、ユーザIDに対応する、図２のステップＳ２７で記憶した精算所５の公開鍵Ｋｐｐｇで暗号化したクレジットカード番号を求める。

【００５６】ステップＳ７５乃至ステップＳ８１は、図２のステップＳ１６乃至ステップＳ２２とそれぞれ同様であるので、その説明は省略する。

【００５７】ステップＳ８２において、センター３の署名部３４は、ステップＳ７２で受信したユーザ機器の署名を付したユーザIDに署名を付し、ステップＳ７２で受信したユーザ機器の署名を付した電子現金発行金額に署名を付し、暗号化部３２は、一時鍵Ｋｔｓｂでユーザ IDおよび電子現金発行金額を暗号化し、通信部３７は、暗号化したユーザIDおよび電子現金発行金額を仮想銀行４に送信する。仮想銀行４の通信部４６は、センター３が送信したユーザIDおよび電子現金発行金額を受信する。

【００５８】ステップＳ８３において、仮想銀行４の復号部４３は、ステップＳ８２で受信したユーザIDおよび電子現金発行金額を一時鍵Ｋｔｓｂで復号し、署名部４４は、電子現金発行金額に付されたセンター３の署名およびユーザ機器１の署名を検証し、電子現金発行金額に改竄がないことを確認する。署名の検証は、図２のステップＳ１５で説明した処理と同様なので、その説明は省略する。署名部４４が電子現金発行金額の改竄を発見した場合、処理は終了する。電子現金発行金額が改竄されていない場合、ステップＳ８４において、口座管理部４５は、ユーザIDに対応する電子現金の金額に、今回の電子現金発行金額を加算する。

【００５９】ステップＳ８５乃至ステップＳ８７は、図２のステップＳ２６乃至ステップＳ２８の処理とそれぞれ同様であり、その説明は省略する。

【００６０】ステップＳ８８において、ユーザ機器１の記憶部１２は、記憶部１２が記憶する電子現金残高に、ステップＳ７２で送信した電子現金発行金額を加算し、記憶する。

【００６１】このように、ユーザ機器１は、仮想銀行４に２回目以降も電子現金を入金することができる。

【００６２】次に、販売店２がセンター３および仮想銀行４に登録する処理を、図５のフローチャートを用いて説明する。ステップＳ９１において、販売店２の通信部２６は、認証局６に販売店情報、口座情報、および販売店２の公開鍵Ｋｐｍを送信する。認証局６は、販売店２の通信部２６が送信したデータを受信する。ステップＳ９２において、認証局６は、受信した販売店情報、口座情報、および販売店２の公開鍵Ｋｐｍに所定のハッシュ関数を適用し、得られたハッシュ値を認証局６の秘密鍵Ｋｓｃａで暗号化して署名を作成し、販売店情報、口座情報、および販売店２の公開鍵Ｋｐｍに付加して証明書を作成し、販売店２に送信する。販売店２の通信部２６は、認証局６が送信したデータを受信する。

【００６３】ステップＳ９３において、販売店２の相互認証部２１は、センター３の相互認証部３１と、相互認証し、販売店２およびセンター３は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｓｍとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ９４において、販売店２の暗号化部２３は、精算所５の公開鍵Ｋｐｐｇで予め記憶している販売店２の口座番号を暗号化する。販売店２の暗号化部２３は、精算所５の公開鍵Ｋｐｐｇで暗号化された口座番号を一時鍵Ｋｔｓｍで更に暗号化し、販売店２の証明書も一時鍵Ｋｔｓｍで

暗号化する。通信部２６は、一時鍵Ｋｔｓｍで暗号化された口座番号および販売店２の証明書をセンター３に送信する。センター３の通信部３７は、販売店２から送信された、一時鍵Ｋｔｓｍで暗号化された口座番号および証明書を受信し、復号部３３は、一時鍵Ｋｔｓｍで暗号化された口座番号および証明書を復号する。

【００６４】ステップＳ９５に進み、センター３の相互認証部３１は、精算所５の相互認証部５１と相互認証し、センター３の相互認証部３１および精算所５の相互認証部５１は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｓｐとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ９６において、センター３の署名部３４は、販売店２の口座番号に署名を付し、暗号化部３２は、販売店２の証明書、およびセンター３の署名を付され、精算所５の公開鍵Ｋｐｐｇで暗号化された口座番号を、一時鍵Ｋｔｓｐで更に暗号化し、通信部３７は、一時鍵Ｋｔｓｐで暗号化されたデータを精算所５に送信する。精算所５の通信部５６は、センター３から送信されたデータを受信する。

【００６５】ステップＳ９７において、精算所５の復号部５３は、センター３から受信したデータを一時鍵Ｋｔｓｐで復号し、精算所５の署名部５４は、証明書に付された認証局６の署名を検証し、証明書に改竄がないことを確認する。署名部３４が証明書の改竄を発見した場合、処理は終了する。証明書が改竄されていない場合、ステップＳ９８に進み、署名部５４は、受信した口座番号にハッシュ関数を適用してハッシュ値を算出し、証明書にあるハッシュ値と一致するかを検証し、口座番号に改竄がないことを確認する。署名部３４が口座番号の改竄を発見した場合、処理は終了する。口座番号に改竄がない場合、ステップＳ９９において、署名部５４は、ステップＳ９８およびステップＳ９８の検証結果に署名を付し、暗号化部５２は、一時鍵Ｋｔｓｐで署名を付した検証結果を暗号化し、通信部５６は、一時鍵Ｋｔｓｐで暗号化した検証結果をセンター３に送信する。センター３の通信部３７は、精算所５が送信した検証結果を受信し、復号部３３は、精算所５から受信した検証結果を一時鍵Ｋｔｓｐで復号する。

【００６６】ステップＳ１００において、センター３の相互認証部３１は、仮想銀行４の相互認証部４１と相互認証し、センター３および仮想銀行４は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｓｂとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ１０１において、センター３の署名部３４は、証明書にセンター３の署名を付し、暗号化部３２は、センター３の署名を付した販売店２の証明書を一時鍵Ｋｔｓｂで暗号化し、通信部３７は、一時鍵Ｋｔｓｂで暗号化された販売店２の証明書を仮想銀行４に送信する。仮想銀行４の通信部４６は、センター３から送信された販売店２の証明書を受信する。

【００６７】ステップＳ１０２において、仮想銀行４の復号部４３は、センター３から受信した販売店２の証明書を一時鍵Ｋｔｓｂで復号し、署名部４４は、販売店２の証明書に付されたセンター３の署名および販売店２の証明書に含まれる認証局６の署名を検証し、販売店２の証明書に改竄がないことを確認する。販売店２の証明書に改竄が発見された場合、処理は終了する。販売店２の証明書に改竄がない場合、ステップＳ１０３において、仮想銀行４の口座管理部４５は、販売店IDを生成し、販売店IDに対応する売り上げ金額を記憶する。

【００６８】ステップＳ１０４乃至ステップＳ１０６の処理は、図２のステップＳ２６乃至ステップＳ２８の処理にそれぞれ同様の処理であるのでその説明は、省略する。

【００６９】ステップＳ１０７において、販売店２の復号部２４は、受信した販売店IDを復号し、記憶部２２は、ステップＳ１０６で受信した販売店IDを記憶する。

【００７０】このように、販売店２は、センター３および仮想銀行４に登録し、販売店IDを記憶する。

【００７１】次に、ユーザ機器１－２からユーザ機器１－１への電子現金の移動を、図６のフローチャートを用いて説明する。ステップＳ１２１において、ユーザ機器１－２の相互認証部１１－２は、ユーザ機器１－１の相互認証部１１－１と、相互認証し、ユーザ機器１－２およびユーザ機器１－１は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｕｕとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ１２２において、ユーザ機器１－２の署名部１５－２は、ユーザにより設定された移動する金額を示すデータに署名を付し、暗号化部１３－２は、移動する金額を示すデータを一時鍵Ｋｔｕｕで暗号化する。ユーザ機器１－２の通信部１６－２は、一時鍵Ｋｔｕｕで暗号化された金額を示すデータをユーザ機器１－１の通信部１６－１に送信する。ユーザ機器１－１の通信部１６－１は、一時鍵Ｋｔｕｕで暗号化された金額を示すデータを受信する。

【００７２】ステップＳ１２３において、ユーザ機器１－１の復号部１４－１は、暗号化された金額を示すデータを一時鍵Ｋｔｕｕで復号し、記憶部１２－１は、記憶している未精算金額に、移動する金額を加算し、記憶する。未精算金額とは、他のユーザ機器１から移動し、受け取った金額の総額を言う。ステップＳ１２４において、ユーザ機器１－１の署名部１５－１は、移動する金額を示すデータに署名を付し、暗号化部１３－１は、移動する金額を示すデータを一時鍵Ｋｔｕｕで暗号化する。ユーザ機器１－１の通信部１６－１は、暗号化した金額を示すデータをユーザ機器１－２の通信部１６－２に送信する。ユーザ機器１－２の通信部１６－２は、暗

号化した金額を示すデータを受信する。

【００７３】ステップＳ１２５において、ユーザ機器１－２の復号部１４－２は、暗号化した金額を示すデータを一時鍵Ｋｔｕｕで復号し、記憶部１２－２は、記憶している未精算金額から、復号した得られた、移動する金額を減じ、記憶する。ステップＳ１２６において、署名部１５－２は、電子現金の移動の終了を示すデータに署名を付し、暗号化部１３－２は、署名を付した電子現金の移動の終了を示すデータを一時鍵Ｋｔｕｕで暗号化し、通信部１６－２は、暗号化された電子現金の移動の終了を示すデータをユーザ機器１－１の通信部１６－１に送信する。ユーザ機器１－１の通信部１６－１は、一時鍵Ｋｔｕｕで暗号化された電子現金の移動の終了を示すデータを受信し、処理は終了する。

【００７４】以上のように、ユーザ機器１－２は、ユーザ機器１－１に電子現金を移動する。

【００７５】図７は、ユーザ機器１－２からユーザ機器１－１への電子現金の移動の他の処理を説明するフローチャートである。ステップＳ１３１において、ユーザ機器１－２の相互認証部１１－２は、ユーザ機器１－１の相互認証部１１－１と、相互認証し、ユーザ機器１－２およびユーザ機器１－１は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｕｕとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ１３２において、ユーザ機器１－２の署名部１５－２は、ユーザにより設定された移動する金額を示すデータに署名を付し、暗号化部１３－２は、センター３の公開鍵Ｋｐｅｓｃでユーザ機器１－２のユーザIDを暗号化し、更に移動する金額を示すデータおよびセンター３の公開鍵Ｋｐｅｓｃで暗号化したユーザ機器１－２のユーザIDを一時鍵Ｋｔｕｕで暗号化する。ユーザ機器１－２の通信部１６－２は、一時鍵Ｋｔｕｕで暗号化した金額を示すデータおよびユーザ機器１－２のユーザIDを、ユーザ機器１－１の通信部１６－１に送信する。ユーザ機器１－１の通信部１６－１は、暗号化した金額を示すデータおよびユーザ機器１－２のユーザIDを受信する。

【００７６】ステップＳ１３３において、ユーザ機器１－１の復号部１４－１は、暗号化した金額を示すデータおよびユーザ機器１－２のユーザIDを一時鍵Ｋｔｕｕで復号し、記憶部１２－１は、記憶している未精算金額に、移動する金額を加算し、得られた金額およびセンター３の公開鍵Ｋｐｅｓｃで暗号化したユーザ機器１－２のユーザIDを、記憶する。

【００７７】ステップＳ１３４乃至ステップＳ１３６の処理は、図６のステップＳ１２４乃至ステップＳ１２６の処理とそれぞれ同様であり、その説明は省略する。

【００７８】図７の処理により、ユーザ機器１－２は、ユーザ機器１－１に電子現金を移動し、ユーザ機器１－１は、移動し現金と共に、ユーザ機器１－２のユーザIDを記憶する。

【００７９】次に、電子現金によるユーザ機器１から販売店２への支払いの処理を、図８のフローチャートを用いて説明する。ステップＳ１５１において、ユーザは、ユーザ機器１の記憶部１２に記憶する電子現金の残高を確認し、購入金額に対して、不足している場合は、図４に示す処理を行い、必要な電子現金の額を記憶させる。ステップＳ１５２において、ユーザ機器１の相互認証部１１は、販売店２の相互認証部２１と、相互認証し、ユーザ機器１および販売店２は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｕｍとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。

【００８０】ステップＳ１５３において、ユーザ機器１の暗号化部１３は、販売店２から購入する購入品の情報（ユーザ機器１の操作により、ユーザが指定した購入品の情報）を、予め記憶部１２に記憶した販売店２の公開鍵Ｋｐｍで暗号化し、ユーザIDを、予め記憶部１２に記憶したセンター３の公開鍵Ｋｐｅｓｃで暗号化し、記憶部１２に記憶した未精算金額を仮想銀行４の公開鍵Ｋｐｖｂで暗号化する。

【００８１】次に、ユーザ機器１の署名部１５は、購入品に関する情報およびユーザIDに署名を付し、仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額に署名を付し、センター３の公開鍵Ｋｐｅｓｃで暗号化したユーザIDに署名を付し、購入金額に署名を付す。ユーザ機器１の暗号化部１３は、販売店２の公開鍵Ｋｐｍで暗号化した購入品に関する情報、センター３の公開鍵Ｋｐｅｓｃで暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名、署名を付した仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額、署名を付したセンター３の公開鍵Ｋｐｅｓｃで暗号化したユーザID、並びに署名を付した購入金額を、一時鍵Ｋｔｕｍで更に暗号化する。ユーザ機器１の通信部１６は、一時鍵Ｋｔｕｍで暗号化された、販売店２の公開鍵Ｋｐｍで暗号化した購入品に関する情報、センター３の公開鍵Ｋｐｅｓｃで暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名、署名を付した仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額、署名を付したセンター３の公開鍵Ｋｐｅｓｃで暗号化したユーザID、並びに署名を付した購入金額を、販売店２の通信部２６に送信し、販売店２の通信部２６は、これらのデータを受信する。

【００８２】ステップＳ１５４において、販売店２の復号部２４は、ステップＳ１５３で受信した、販売店２の公開鍵Ｋｐｍで暗号化した購入品に関する情報、センター３の公開鍵Ｋｐｅｓｃで暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名、署名を付した仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額、署名を付したセンター３の公開鍵Ｋｐｅｓｃで暗号化したユーザID、並びに署名を付した購入金額を、一時

鍵Ｋｔｕｍで復号する。署名部３４は、購入品に関する情報およびユーザIDに対するユーザ機器１の署名を確認し、改竄があったかどうかを確認し、改竄があったと判定された場合、処理は、終了する。改竄がないと判定された場合、復号部２４は、販売店２の公開鍵Ｋｐｍで暗号化した購入品に関する情報を、販売店２の秘密鍵Ｋｓｍで復号する。また、購入品に対する情報、金額より、購入品に対する金額の確認と、販売店２の公開鍵Ｋｐｍで暗号化した購入品に関する情報、センター３の公開鍵Ｋｐｅｓｃで暗号化したユーザID、購入品に関する情報およびユーザIDに対する署名より、ユーザID、購入品の組が正しいことを確認する。

【００８３】ステップＳ１５５において、販売店２の相互認証部２１は、センター３の相互認証部３１と相互認証し、販売店２およびセンター３は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｓｍとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。

【００８４】ステップＳ１５６において、販売店２の暗号化部２３は、記憶部２２に記憶している販売店２の販売店IDを、ステップＳ１５５で得られたセンター３の公開鍵Ｋｐｅｓｃで暗号化し、署名部２５は、センター３の公開鍵Ｋｐｅｓｃで暗号化した販売店IDに署名を付し、ステップＳ１５４で復号した購入金額に対するユーザ機器１の署名に署名を付す。暗号化部３２は、ステップ１５２で得られたユーザの証明書、センター３の公開鍵Ｋｐｅｓｃで暗号化し、販売店の署名およびユーザ機器１の署名を付したユーザID、仮想銀行４の公開鍵Ｋｐｖｂで暗号化し、ユーザ機器１の署名を付した未精算金額、署名を付したセンター３の公開鍵Ｋｐｅｓｃで暗号化した販売店ID、並びに署名を付した購入金額を、一時鍵Ｋｔｓｍで暗号化し、通信部２６は、それらのデータをセンター３の通信部３７に送信する。センター３の通信部３７は、一時鍵Ｋｔｓｍで暗号化された、ステップ１５２で得られたユーザの証明書、センター３の公開鍵Ｋｐｅｓｃで暗号化し、販売店の署名およびユーザ機器１の署名を付したユーザID、仮想銀行４の公開鍵Ｋｐｖｂで暗号化し、ユーザ機器１の署名を付した未精算金額、署名を付したセンター３の公開鍵Ｋｐｅｓｃで暗号化した販売店ID、並びに署名を付した購入金額を受信する。

【００８５】ステップＳ１５７において、センター３の復号部３３は、ステップＳ１５６で受信した、ユーザの証明書、センター３の公開鍵Ｋｐｅｓｃで暗号化し販売店の署名およびユーザ機器１の署名を付したユーザID、仮想銀行４の公開鍵Ｋｐｖｂで暗号化し、ユーザ機器１の署名を付した未精算金額、署名を付したセンター３の公開鍵Ｋｐｅｓｃで暗号化した販売店ID、並びに署名を付した購入金額を一時鍵Ｋｔｓｍで復号する。署名部３４は、購入金額へのユーザ機器１の署名および販売店２の署名、ユーザIDに付した販売店の署名およびユーザ機器１の署名、並びに販売店IDへの販売店２の署名を検証し、購入金額、ユーザID、および販売店IDに改竄がないことを確認する。署名部３４が購入金額、ユーザID、または販売店IDのいずれかに改竄を発見した場合、処理は終了する。購入金額、ユーザID、および販売店IDが改竄されてない場合、ステップＳ１５８において、センター３の相互認証部３１は、仮想銀行４の相互認証部４１と相互認証し、センター３および仮想銀行４は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｓｂとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。

【００８６】ステップＳ１５９において、センター３の署名部３４は、ユーザID、販売店ID、購入金額、仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額に署名を付し、センター３の暗号化部３２は、ユーザID、販売店ID、購入金額、仮想銀行の公開鍵Ｋｐｖｂで暗号化した未精算金額、および署名を一時鍵Ｋｔｓｂで暗号化し、通信部３７は、暗号化したユーザID、販売店ID、購入金額、仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額、および署名を、仮想銀行４の通信部４６に送信する。仮想銀行４の通信部４６は、暗号化したユーザID、販売店ID、購入金額、仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額、および署名を、受信する。

【００８７】ステップＳ１６０において、仮想銀行４の復号部４３は、暗号化したユーザID、販売店ID、購入金額、仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額、およびセンター３の署名を一時鍵Ｋｔｓｂで復号する。署名部４４は、センター３の署名を検証し、ユーザID、販売店ID、購入金額、および仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額に改竄がないことを確認する。署名部４４が、改竄を発見した場合、処理は終了する。ユーザID、販売店ID、購入金額、および仮想銀行４の公開鍵Ｋｐｖｂで暗号化した未精算金額のいずれにも改竄がない場合、口座管理部４５は、販売店IDに対応する売り上げ金額に購入金額を加算する。ステップＳ１６１において、口座管理部４５は、ユーザIDに対応する残高から購入金額を減じ、ユーザIDに対応する残高に未精算金額を加算し、記憶する。

【００８８】ステップＳ１６２において、仮想銀行４の暗号化部４２は、ステップＳ１６１で記憶したユーザIDに対応する残高をユーザの公開鍵Ｋｐｕで暗号化し、署名部４４は、購入金額およびユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高に署名し、通信部４６は、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、および署名をセンター３の通信部３７に送信し、センター３の通信部３７は、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、および署名を受信する。

【００８９】ステップＳ１６３において、センター３の

復号部３３は、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、および仮想銀行４の署名を復号し、センター３の署名部３４は、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、および仮想銀行４の署名に、センター３の署名を付し、暗号化部３２は、センター３の署名を付した、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、および仮想銀行４の署名を一時鍵Ｋｔｓｍで暗号化する。通信部３７は、販売店２の通信部２６に、一時鍵Ｋｔｓｍで暗号化した、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、仮想銀行４の署名、およびセンター３の署名を送信する。販売店２の通信部２６は、これらのデータを受信する。

【００９０】ステップＳ１６４において、販売店２の復号部２４は、受信した購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、仮想銀行４の署名、およびセンター３の署名を一時鍵Ｋｔｓｍで復号し、署名部２５は、仮想銀行４の署名、およびセンター３の署名を検証し、受信した購入金額、およびユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高に改竄がないことを確認する。署名部２５が、改竄を発見した場合、処理は終了する。受信した購入金額、およびユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高のいずれにも改竄がない場合、ステップＳ１６５に進み、署名部２５は、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、仮想銀行４の署名、およびセンター３の署名に販売店２の署名を付し、暗号化部２３は、一時鍵Ｋｔｕｍで購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、仮想銀行４の署名、センター３の署名、および販売店２の署名を暗号化し、通信部２６は、暗号化された購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、仮想銀行４の署名、センター３の署名、および販売店２の署名をユーザ機器１の通信部１６に送信する。ユーザ機器１の通信部１６は、購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、仮想銀行４の署名、センター３の署名、および販売店２の署名を受信する。

【００９１】ステップＳ１６６において、ユーザ機器１の復号部１４は、受信した購入金額、ユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高、仮想銀行４の署名、センター３の署名、および販売店２の署名を一時鍵Ｋｔｕｍで復号し、署名部１５は、仮想銀行４の署名、センター３の署名、および販売店２の署名を検証し、受信した購入金額、およびユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高に改竄がないことを確認する。署名部１５が、改竄を発見した場合、処理は終了する。受信した購入金額、およびユーザの公開鍵Ｋｐｕで暗号化したユーザIDに対応する残高のいずれにも改竄がない場合、記憶部１２は、受信した残高が、処理開始前から記憶部１２に記憶する残高より購入金額を減じ、ステップＳ１５３で送信した未精算金額を加えた金額と等しいかを確認し、受信した残高が、処理開始前から記憶部１２に記憶する残高より購入金額を減じ、ステップＳ１５３で送信した未精算金額を加えた金額と等しい場合、残高を更新して記憶し、未精算金額を０とし、処理は終了する。受信した残高が、処理開始前から記憶部１２に記憶する残高より購入金額を減じ、ステップＳ１５３で送信した未精算金額を加えた金額と等くない場合、処理は終了する。

【００９２】以上のように、ユーザ機器１は、仮想銀行４を介して、販売店２に支払いを行う。

【００９３】図９のフローチャートを用いて、販売店２の口座への売上金の入金の処理を説明する。ステップＳ１８１において、販売店２の相互認証部２１は、センター３の相互認証部３１と、相互認証し、販売店２およびセンター３は、図３のステップＳ５４およびステップＳ５７の乱数の連接Ｒ２‖Ｒ３を一時鍵Ｋｔｓｍとして共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ１８２において、販売店２の暗号化部２３は、一時鍵Ｋｔｓｍで、図５のステップＳ１０７で記憶部２２に記憶している販売店２の販売店IDを暗号化する。販売店２の署名部２５は、暗号化した販売店IDに署名を付し、暗号化部２３は、販売店IDおよび署名を一時鍵Ｋｔｓｍで暗号化する。通信部２６は、一時鍵Ｋｔｓｍで暗号化された販売店IDおよび署名をセンター３の通信部３７に送信し、センター３の通信部３７は、販売店IDおよび署名を受信する。

【００９４】ステップＳ１８３において、センター３の復号部３３は、一時鍵Ｋｔｓｍで暗号化された販売店IDおよび署名を復号し、署名部３４は、復号して得られた、販売店IDに付された署名を検証し、販売店IDが改竄されていないことを確認する。販売店IDに改竄が発見されれば、処理は終了する。販売店IDに改竄が発見されない場合、ステップＳ１８４において、センター３の相互認証部３１は、仮想銀行４の相互認証部４１と相互認証し、センター３および仮想銀行４は、一時鍵Ｋｔｓｂを共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ１８５において、センター３の署名部３４は、ステップＳ１８３で確認された販売店IDに署名を付し、暗号化部３２は、販売店IDおよび署名を一時鍵Ｋｔｓｂで暗号化する。通信部３７は、一時鍵Ｋｔｓｂで暗号化された販売店IDおよび署名を仮想銀行４の通信部４６に送信し、仮想銀行４の通信部４６は、販売店IDおよび署名を受信する。

【００９５】ステップＳ１８６において、仮想銀行４の復号部４３は、一時鍵Ｋｔｓｂで暗号化された販売店IDおよび署名を復号し、署名部４４は、復号して得られた、販売店IDに付された署名を検証し、販売店IDが改竄されていないことを確認する。販売店IDに改竄が発見さ

れれば、処理は終了する。販売店IDに改竄が発見されなければ、口座管理部４５は、口座管理部４５に記憶する販売店IDに対応する売り上げ金額をクリアする。ステップＳ１８７において、署名部４４は、口座管理部４５に記憶する販売店IDに対応する売り上げ金額（クリアする前の売り上げ金額）に署名を付し、暗号化部４２は、売り上げ金額および署名を一時鍵Ｋｔｓｂで暗号化する。通信部４６は、一時鍵Ｋｔｓｂで暗号化された売り上げ金額および署名をセンター３の通信部３７に送信し、センター３の通信部３７は、売り上げ金額および署名を受信する。

【００９６】ステップＳ１８８において、センター３の相互認証部３１は、精算所５の相互認証部５１と相互認証し、センター３および精算所５は、一時鍵Ｋｔｓｐを共有する。相互認証の手続は、図３の処理と同様であるので説明は省略する。ステップＳ１８９において、センター３の署名部３４は、ステップＳ１８７で仮想銀行４から受信した売り上げ金額に署名を付し、暗号化部３２は、ステップＳ１８１の相互認証の処理で販売店２から受信した販売店の証明書、図５のステップ１０５で販売店管理部３６に記憶した、精算所５の公開鍵Ｋｐｐｇで暗号化した販売店IDに対応する口座番号、およびセンター３の署名を付した売り上げ金額を一時鍵Ｋｔｓｐで暗号化する。通信部３７は、一時鍵Ｋｔｓｐで暗号化した、販売店の証明書、販売店IDに対応する口座番号、および売り上げ金額を、精算所５の通信部５６に送信する。精算所５の通信部５６は、一時鍵Ｋｔｓｐで暗号化した、販売店の証明書、販売店IDに対応する口座番号、および売り上げ金額を受信する。

【００９７】ステップＳ１９０において、精算所５の復号部５３は、販売店の証明書、販売店IDに対応する口座番号、および売り上げ金額を復号し、署名部５４は、復号した売り上げ金額に改竄がないことを確認し、改竄が発見されれば、処理は終了する。改竄が発見されなければ、精算部５５は、売り上げ金額に相当する金額を販売店IDに対応する口座番号に入金する処理を、銀行に実行させる。ステップＳ１９１において、署名部５４は、ステップＳ１９０の処理の結果を示すデータに署名を付し、通信部５６は、入金処理の結果を示すデータおよび署名をセンター３の通信部３７に送信する。センター３の通信部３７は、入金処理の結果を示すデータおよび署名を受信する。

【００９８】ステップＳ１９２において、センター３の復号部３３は、入金処理の結果を示すデータおよび署名を復号し、署名部３４は、入金処理の結果を示すデータに改竄がないことを確認し、改竄が発見されれば、処理は終了する。改竄が発見されなければ、署名部３４は、入金処理の結果を示すデータに署名を付し、通信部３７は、入金処理の結果を示すデータおよび署名を販売店２の通信部２６に送信する。販売店２の通信部２６は、入金処理の結果を示すデータおよび署名を受信し、販売店２の復号部２４は、入金処理の結果を示すデータおよび署名を復号し、署名部２５は、入金処理の結果を示すデータに改竄がないことを確認し、記憶部２２は、入金処理の結果を示すデータを記憶し、処理は終了する。

【００９９】以上のように、販売店２の口座への売り上げ金の入金が処理される。

【０１００】このように、各装置での利用者の識別をユーザIDで行う。個人情報は各装置が把握しておらず、不正検出時には、センター３がユーザIDを基に精算所５の公開鍵Ｋｐｐｇで暗号化された口座情報を求め、精算所５に対して口座情報の開示を要求する。それを基に、認証局６、クレジットカード会社７、または銀行８に対して個人情報の特定を行う。その場合、どういうケースで各装置が情報を開示するかという制御ができ、またそれらを参照した履歴も管理できるため、不必要に個人情報が開示されることはない。

【０１０１】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０１０２】なお、上記したような処理を行うコンピュータプログラムをユーザ機器に提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０１０３】

【発明の効果】請求項１に記載の電子現金システムによれば、口座管理装置が、利用者を識別する情報、および前払いの代金を基にした利用者の利用金額を記憶し、決済処理装置が、支払機関に決済を指示し、制御装置が、利用者を識別する情報、および決済処理装置の公開鍵で暗号化された利用者の支払機関の口座番号を管理し、利用者を特定する情報を基に、口座管理装置が記憶する利用者の前払いの残高の変更を指示し、支払い機関の口座番号を基に、決済処理装置に決済の実行を指示するようにしたので、利用者が特殊な装置を管理する必要がなく、安全に電子現金の利用ができ、個人の情報および個人の購入情報を各装置が不必要に把握できず、不正の検出が可能で、金銭の流通が管理できる。

【図面の簡単な説明】

【図１】本発明を適用した電子現金システムの構成を表す図である。

【図２】仮想銀行４に初めて入金し、ユーザIDを登録するときの処理を説明するフローチャートである。

【図３】相互認証の処理を説明するフローチャートである。

【図４】ユーザ機器１が、仮想銀行４に２回目以降に入金するときの処理を説明するフローチャートである。

【図５】販売店２がセンター３および仮想銀行４に登録する処理を説明するフローチャートである。

【図６】ユーザ機器１－２からユーザ機器１－１への電子現金の移動する処理を説明するフローチャートである。

【図７】ユーザ機器１－２からユーザ機器１－１への電子現金の移動する処理を説明するフローチャートである。

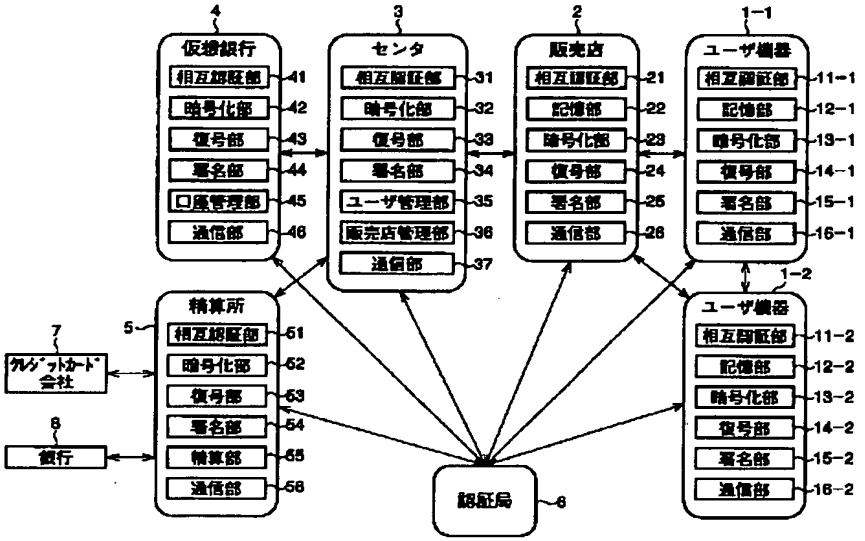
【図８】ユーザ機器１から販売店２への支払いの処理を説明するフローチャートである。

【図９】販売店２の口座への売上金の入金の処理を説明するフローチャートである。

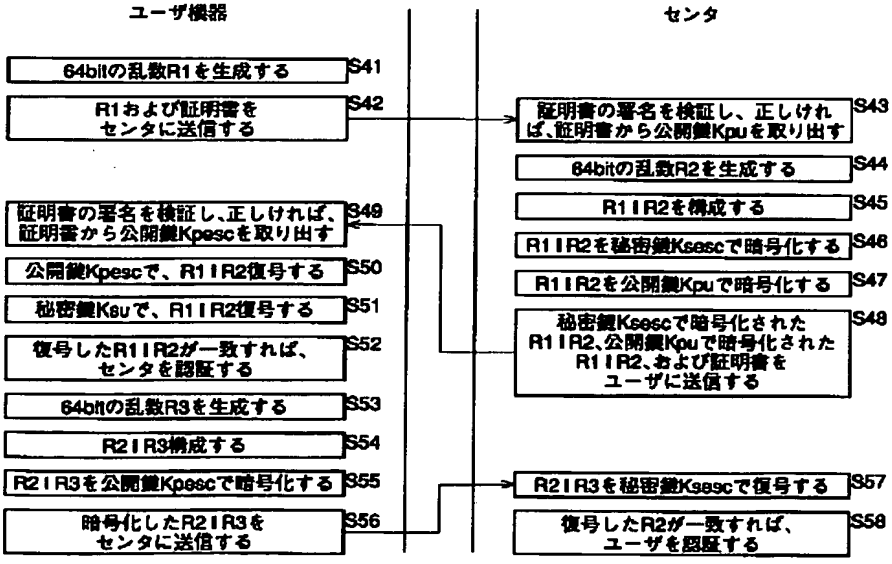
【符号の説明】

１，１－１，１－２　ユーザ機器，　２　販売店，　３　センター，　４　仮想銀行，　５　精算所，　３５　ユーザ管理部，　３７　通信部，　４５　口座管理部，　５５　精算部

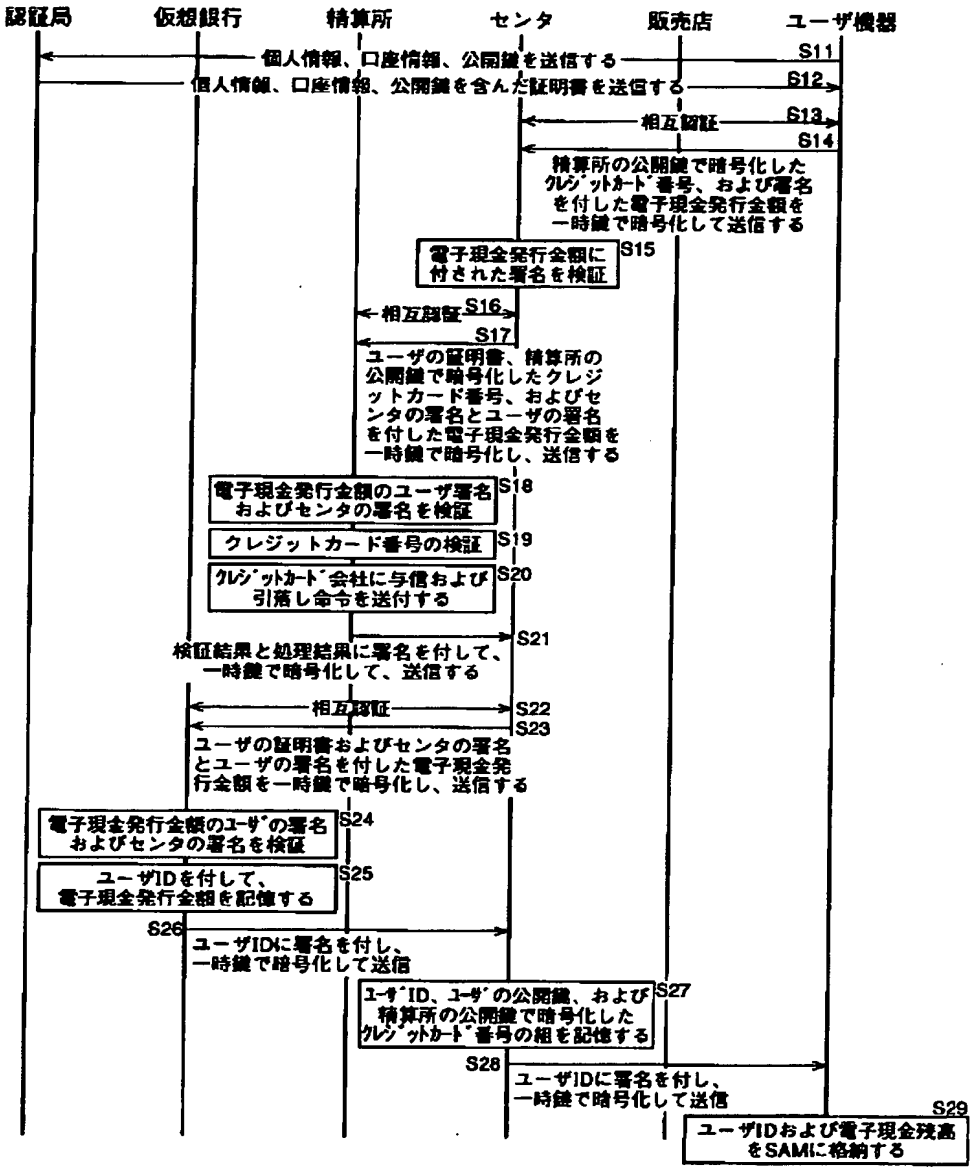
【図１】



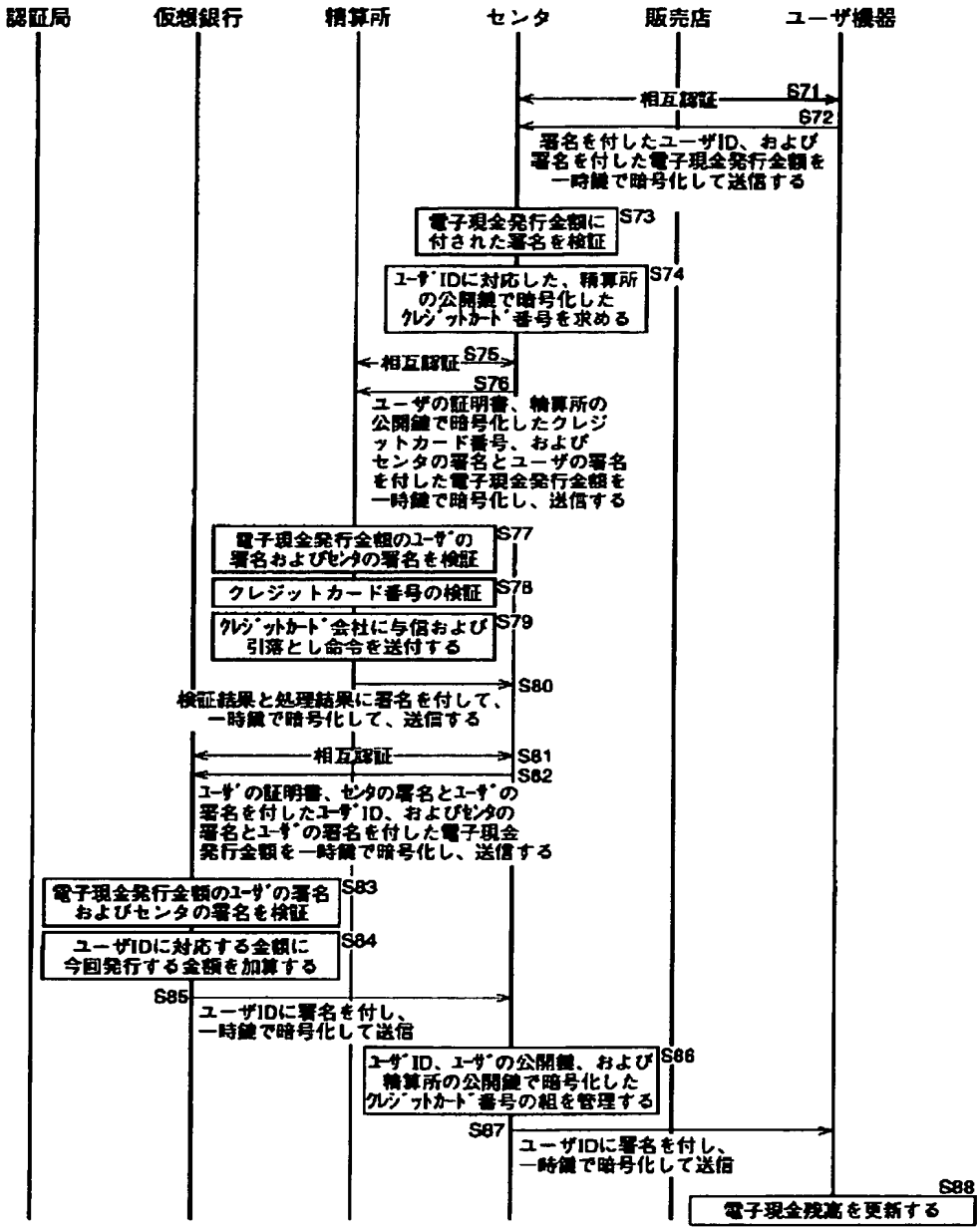
【図３】



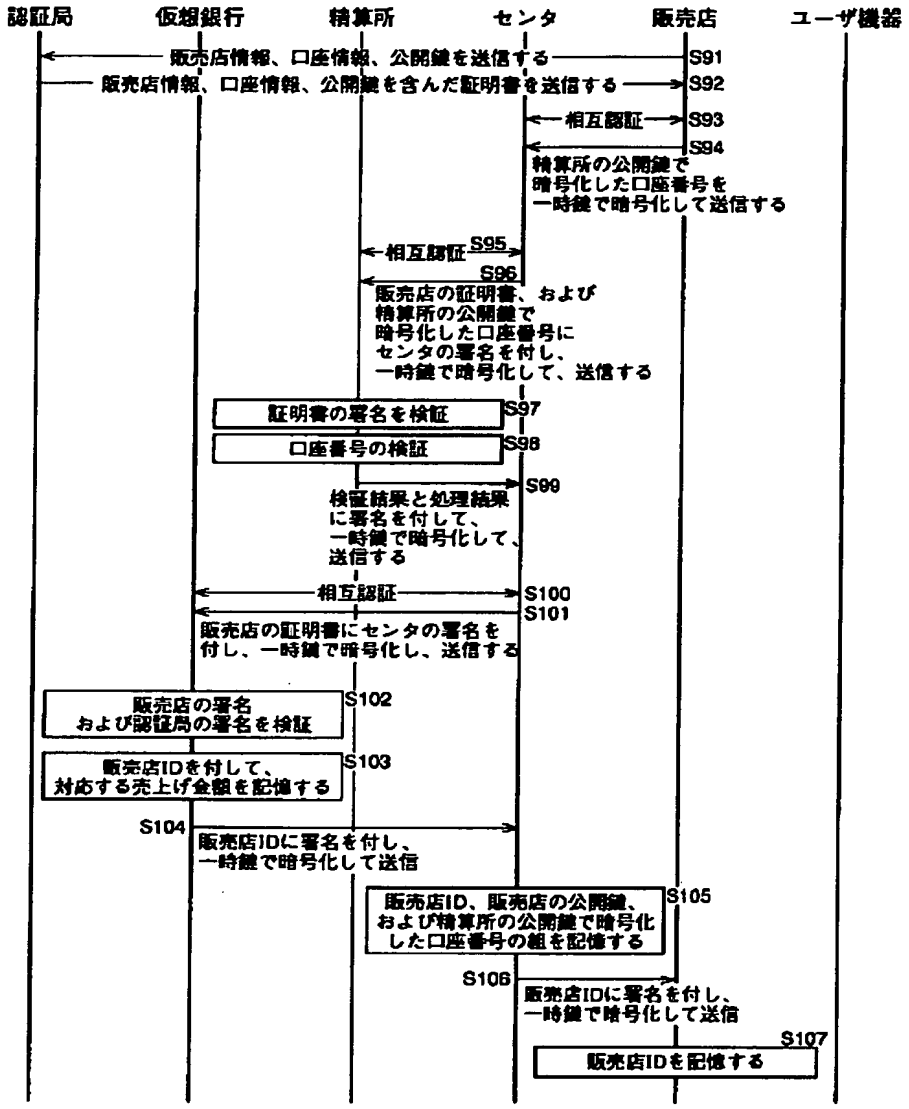
【図２】


認証局
仮想銀行
精算所
センタ
販売店
ユーザ機器
個人情報、口座情報、公開鍵を送信する
S11
個人情報、口座情報、公開鍵を含んだ証明書を送信する
S12
相互認証
S13
S14
精算所の公開鍵で暗号化したクレジットカード番号、および署名を付した電子現金発行金額を一時鍵で暗号化して送信する
電子現金発行金額に付された署名を検証
S15
相互認証
S16
S17
ユーザの証明書、精算所の公開鍵で暗号化したクレジットカード番号、およびセンタの署名とユーザの署名を付した電子現金発行金額を一時鍵で暗号化し、送信する
電子現金発行金額のユーザ署名およびセンタの署名を検証
S18
クレジットカード番号の検証
S19
クレジットカード会社に与信および引落し命令を送付する
S20
S21
検証結果と処理結果に署名を付して、一時鍵で暗号化して、送信する
相互認証
S22
S23
ユーザの証明書およびセンタの署名とユーザの署名を付した電子現金発行金額を一時鍵で暗号化し、送信する
電子現金発行金額のユーザの署名およびセンタの署名を検証
S24
ユーザIDを付して、電子現金発行金額を記憶する
S25
S26
ユーザIDに署名を付し、一時鍵で暗号化して送信
ユーザID、ユーザの公開鍵、および精算所の公開鍵で暗号化したクレジットカード番号の組を記憶する
S27
S28
ユーザIDに署名を付し、一時鍵で暗号化して送信
S29
ユーザIDおよび電子現金残高をSAMに格納する

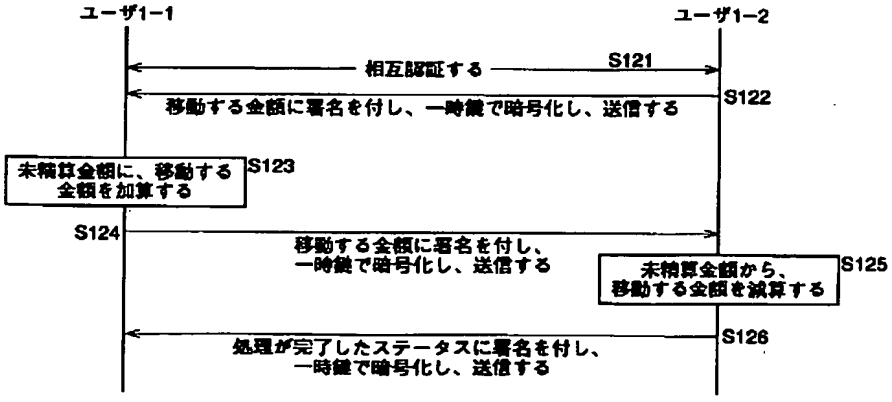
【図４】


認証局
仮想銀行
精算所
センタ
販売店
ユーザ機器
相互認証
S71
S72
署名を付したユーザID、および
署名を付した電子現金発行金額を
一時鍵で暗号化して送信する
電子現金発行金額に
付された署名を検証
S73
ユーザIDに対応した、精算所
の公開鍵で暗号化した
クレジットカード番号を求める
S74
相互認証
S75
S76
ユーザの証明書、精算所の
公開鍵で暗号化したクレジ
ットカード番号、および
センタの署名とユーザの署名
を付した電子現金発行金額を
一時鍵で暗号化し、送信する
電子現金発行金額のユーザの
署名およびセンタの署名を検証
S77
クレジットカード番号の検証
S78
クレジットカード会社に与信および
引落とし命令を送付する
S79
S80
検証結果と処理結果に署名を付して、
一時鍵で暗号化して、送信する
相互認証
S81
S82
ユーザの証明書、センタの署名とユーザの
署名を付したユーザID、およびセンタの
署名とユーザの署名を付した電子現金
発行金額を一時鍵で暗号化し、送信する
電子現金発行金額のユーザの署名
およびセンタの署名を検証
S83
ユーザIDに対応する金額に
今回発行する金額を加算する
S84
S85
ユーザIDに署名を付し、
一時鍵で暗号化して送信
ユーザID、ユーザの公開鍵、および
精算所の公開鍵で暗号化した
クレジットカード番号の組を管理する
S86
S87
ユーザIDに署名を付し、
一時鍵で暗号化して送信
S88
電子現金残高を更新する

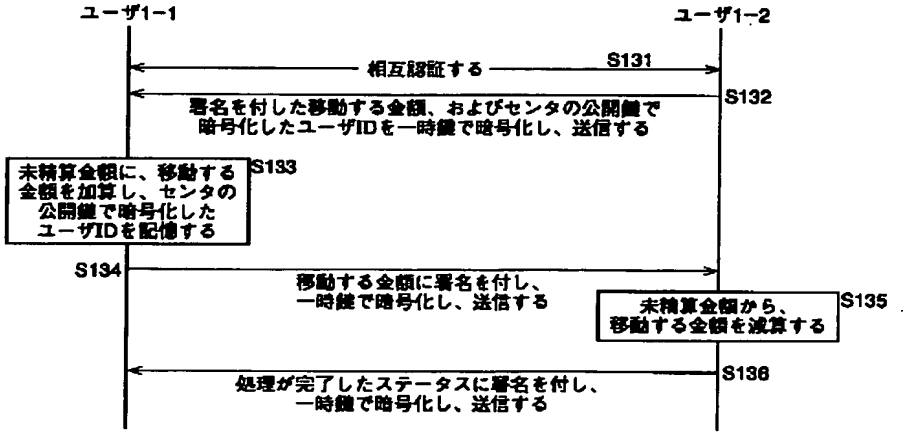
【図５】


認証局
仮想銀行
精算所
センタ
販売店
ユーザ機器
販売店情報、口座情報、公開鍵を送信する
S91
販売店情報、口座情報、公開鍵を含んだ証明書を送信する
S92
相互認証
S93
S94
精算所の公開鍵で
暗号化した口座番号を
一時鍵で暗号化して送信する
相互認証
S95
S96
販売店の証明書、および
精算所の公開鍵で
暗号化した口座番号に
センタの署名を付し、
一時鍵で暗号化して、送信する
証明書の署名を検証
S97
口座番号の検証
S98
S99
検証結果と処理結果
に署名を付して、
一時鍵で暗号化して、
送信する
相互認証
S100
S101
販売店の証明書にセンタの署名を
付し、一時鍵で暗号化し、送信する
販売店の署名
および認証局の署名を検証
S102
販売店IDを付して、
対応する売上げ金額を記憶する
S103
S104
販売店IDに署名を付し、
一時鍵で暗号化して送信
販売店ID、販売店の公開鍵、
および精算所の公開鍵で暗号化
した口座番号の組を記憶する
S105
S106
販売店IDに署名を付し、
一時鍵で暗号化して送信
S107
販売店IDを記憶する

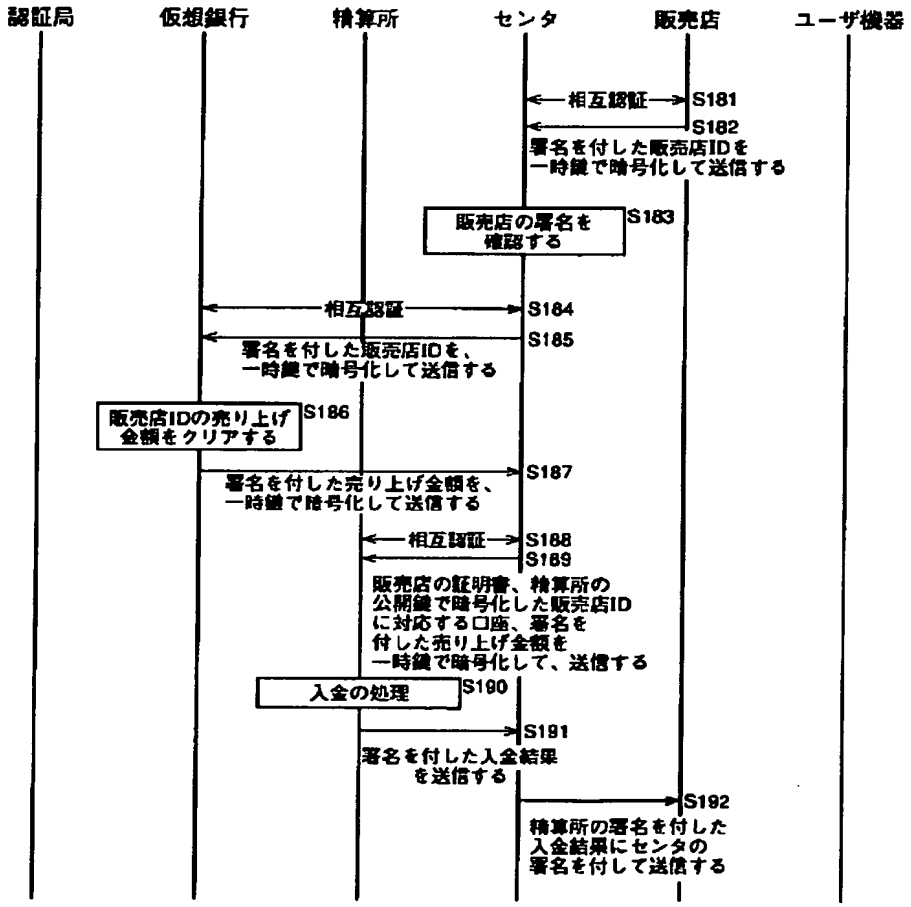
【図６】


ユーザ1−1
ユーザ1−2
相互認証する
S121
S122
移動する金額に署名を付し、一時鍵で暗号化し、送信する
未精算金額に、移動する
金額を加算する
S123
S124
移動する金額に署名を付し、
一時鍵で暗号化し、送信する
未精算金額から、
移動する金額を減算する
S125
S126
処理が完了したステータスに署名を付し、
一時鍵で暗号化し、送信する

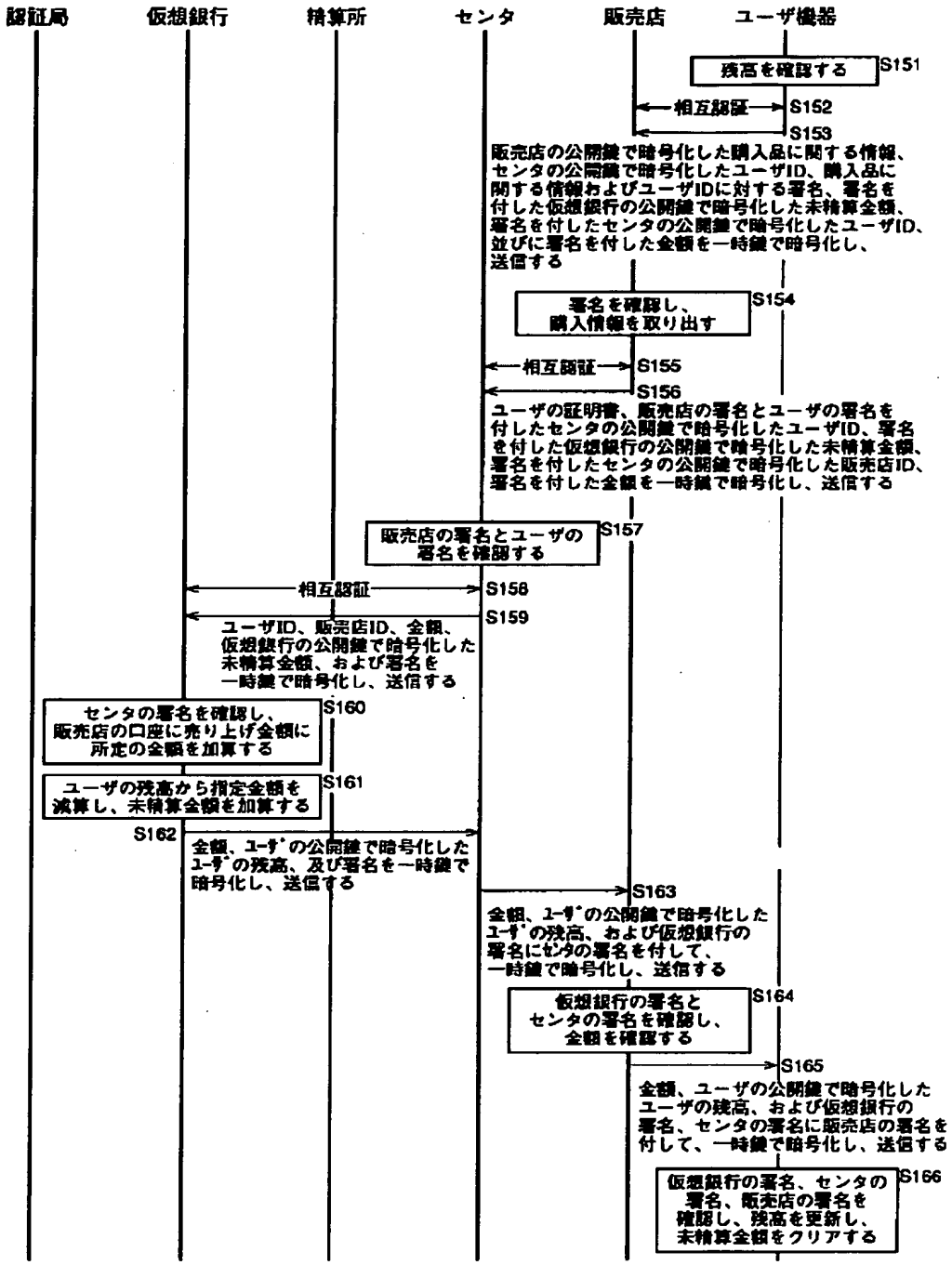
【図７】


ユーザ1−1
ユーザ1−2
相互認証する
S131
S132
署名を付した移動する金額、およびセンタの公開鍵で暗号化したユーザIDを一時鍵で暗号化し、送信する
未精算金額に、移動する金額を加算し、センタの公開鍵で暗号化したユーザIDを記憶する
S133
S134
移動する金額に署名を付し、一時鍵で暗号化し、送信する
未精算金額から、移動する金額を減算する
S135
S136
処理が完了したステータスに署名を付し、一時鍵で暗号化し、送信する

【図９】


認証局
仮想銀行
精算所
センタ
販売店
ユーザ機器
相互認証
S181
S182
署名を付した販売店IDを一時鍵で暗号化して送信する
販売店の署名を確認する
S183
相互認証
S184
S185
署名を付した販売店IDを、一時鍵で暗号化して送信する
販売店IDの売り上げ金額をクリアする
S186
S187
署名を付した売り上げ金額を、一時鍵で暗号化して送信する
相互認証
S188
S189
販売店の証明書、精算所の公開鍵で暗号化した販売店IDに対応する口座、署名を付した売り上げ金額を一時鍵で暗号化して、送信する
入金の処理
S190
S191
署名を付した入金結果を送信する
S192
精算所の署名を付した入金結果にセンタの署名を付して送信する

【図８】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
G09C 1/00	660	G06F 15/30	L	
		G07D 9/00	476	

Fターム(参考)　3E040 BA20 CA14 CA16 DA01
5B049 AA05 BB46 CC36 CC39 EE03
EE09 EE23 EE24 GG04 GG07
GG10
5B055 CB09 EE02 EE03 EE27 FA01
FA05 HA02 HA04 HA12 HB06
HC04 JJ05 KK01 KK09 KK19